CLAIMS

1. An authentication system suitable for automatically providing authentication to a user at a client node, the user providing a user secret and requesting access to network resources resident at one or more server nodes in a distributed network system, said authentication system comprising:

a local application program interface for receiving the user secret, said local application program interface in communication with a requested network resource;

a cryptography service node including means for providing a common key and algorithm, and means for providing a client/server session key and algorithm; and

an authentication database in communication with said local application program interface and with said cryptography service node, said authentication database including

an authentication secret associated with the user;

means for encrypting said authentication secret using said common key and algorithm; and

means for encrypting said common key using said client/server session key and algorithm.

2. The authentication system of claim 1 further comprising means for encrypting and decrypting said authentication secret using a secret store key and algorithm.

3. The authentication system of claim 1 further comprising,

a network resource identifier associated with said requested network resource; and

a network policy associated with the user and with said network resource identifier.

4. The authentication system of claim 1 wherein said authentication database further comprises,

a second network resource identifier associated with a second network resource;

a second authentication secret associated with the user; and

a second network policy associated with the user and with said second network resource identifier.

5. The authentication system of claim 4 wherein said authentication database further comprises means for encrypting and decrypting said second authentication secret using said secret store key and algorithm.

6. The authentication system of claim 4 wherein said authentication database further comprises means for encrypting and decrypting said second authentication secret using a second secret store key and algorithm.

7. The authentication system of claim 1 wherein said cryptography service further comprises means for generating an authentication secret from the user secret.

8. The authentication system of claim 1 wherein said common key comprises a symmetric key.

9. A method for automatically authenticating a user at a network client node in a distributed network system in response to a user request for access to network resources resident in one or more server nodes, said authentication method comprising the steps of:

providing a network resource identifier, a network resource policy, and an authentication secret to an authentication database, said network resource identifier associated with the requested network resource;

retrieving said authentication secret in response to said user request, said authentication secret associated with the user and with said network resource identifier;

encrypting said authentication secret with a common key and algorithm;

encrypting said common key and algorithm with a client/server session key and algorithm; and

providing said encrypted authentication secret and said encrypted common key to the client node.

10. The method of claim 9 further comprising the steps of:

decrypting said encrypted common key using said client/server session key;

decrypting said encrypted authentication secret using said decrypted common key and algorithm; and

providing said decrypted authentication secret to the requested network resource.

11. The method of claim 9 further comprising the step of accessing said network resource policy prior to said step of retrieving said authentication secret, said network resource policy associated with the user and with said network resource identifier.

12. The method of claim 9 further comprising the steps of:

obtaining a list of client algorithms supported by the client node;

obtaining a list of server algorithms supported by the server node;

comparing said list of client algorithms with said list of server algorithms so as to determine the strongest algorithm common to both said list of client algorithms and said list of server algorithms; and

using said strongest algorithm as said common key and algorithm.

13. The method of claim 9 wherein said common key comprises a symmetric key.

14. The method of claim 9 further comprising the steps of:

negotiating the strongest common algorithm between server and client node; and

using said strongest algorithm as said client/server session key and algorithm.